Infogressive, Inc.
Aggressive Information Security

2011 Nebraska Cyber Security Conference

Brandon Harms

CISSP, CEH, GPEN, CCNP, FCNSP

Security Consultant

Infogressive, Inc.
Aggressive Information Security

SANS 20 CRITICAL SECURITY CONTROLS VERSION 3.0

"Offense Must Inform Defense"

Infogressive, Inc.
Aggressive Information Security

Collaboration between members of:

FBI, DoD, Civilian, Federal

Maps directly to:

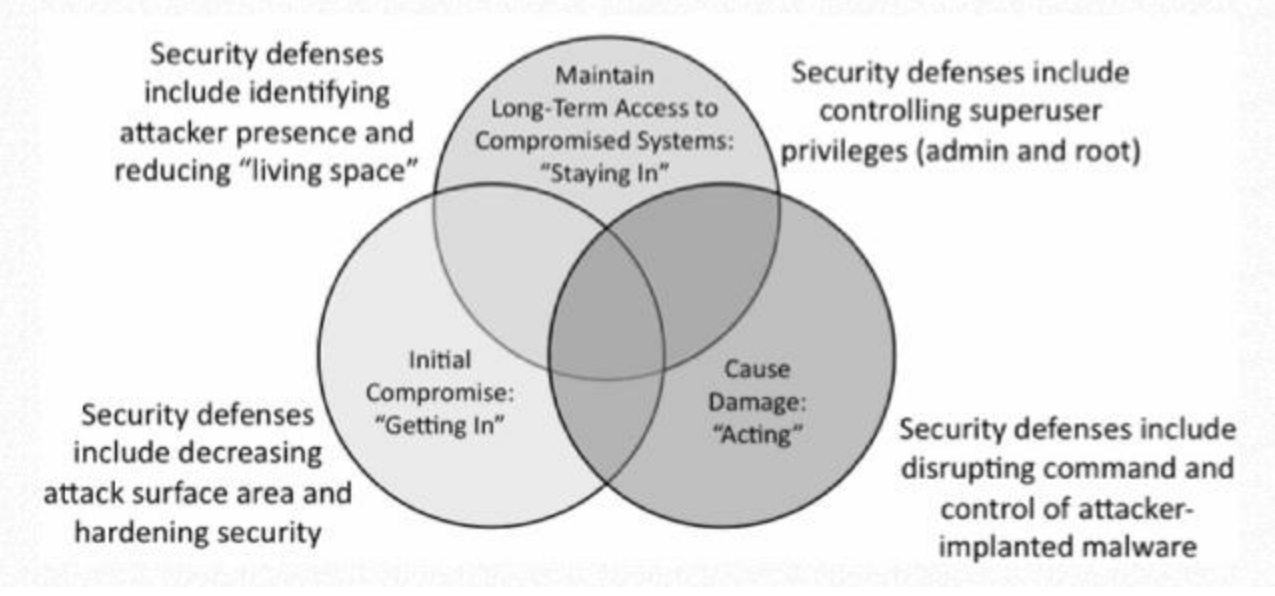
NIST Special Publication 800-53, Rev 3, Priority 1 controls.

http://www.sans.org/critical-security-controls/

How these controls can help

- *Effective in Blocking:*
  - Currently known high-priority attacks
  - Attack types expected in the near future.

Computer Attacker Activities and Associated Defenses



Attackers are continually scanning for new systems

- Critical Control 1
  - Inventory of Authorized and Unauthorized Devices
- Deploy an automated asset inventory discovery tool

Attackers continually scan for vulnerable software & Attackers distribute hostile content on websites

- Critical Control 2
  - Inventory of Authorized and Unauthorized Software

- Devise a list of authorized software.

Attackers use currently infected or compromised machines

- Critical Control 3
  - Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- Strict configuration management should be followed

Attackers exploit “temporary exceptions”

- Critical Control 4
  - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Change Control for Network Devices

Attackers exploit boundary systems

- Critical Control 5
  - Boundary Defense

- Deploy network-based IDS sensors
- Organizations should limit access to known malicious IP addresses

Attackers remain undetected due to a lack of logging and log review

- Critical Control 6
  - Maintenance, Monitoring, and Analysis of Audit Logs
- Validate audit log settings & run biweekly reports

Attackers exploit weak application software

- Critical Control 7
  - Application Software Security
- Organizations should deploy web application firewalls

Attackers gain administrative control

- Critical Control 8
  - Controlled Use of Administrative Privileges
- Inventory all admin passwords
- Before deploying new devices change all default passwords

Attackers gain access to sensitive documents

- Critical Control 9
  - Controlled Access Based on the Need to Know
- Establish a multi-level data identification and classification scheme
- Ensure that file shares have defined controls

Attackers exploit new vulnerabilities

- Critical Control 10
  - Continuous Vulnerability Assessment and Remediation
- At minimum run automated vulnerability scanning tools weekly

Attackers compromise inactive user accounts

- Critical Control 11
  - Account Monitoring and Control
- Regularly monitor and review all system accounts
- Maintain stringent password rules

Attackers use malicious code

- Critical Control 12
  - Malware Defenses
- Send malware detection events to event log servers
- Scan email attachments
- Employ auto update features

Attackers scan for remotely accessible services on target systems

- Critical Control 13
  - Limitation and Control of Network Ports, Protocols, and Services
- Host-based firewalls or port filtering tools should be applied on end systems.
- Automated port scans should be performed on a regular basis

Attackers exploit wireless access points

- Critical Control 14
  - Wireless Device Control
- Ensure that all wireless access points are manageable
- Detect wireless access points connected to the wired network

Attackers gain access to internal enterprise systems

- Critical Control 15
  - Data Loss Prevention
- Deploy approved hard drive encryption software to mobile machines
- Monitor for certain sensitive information

Attackers exploit poorly designed network architectures

- Critical Control 16
  - Secure Network Engineering
- Use minimum of a 3-Tier Architecture
- Utilize private networks

Attackers compromise target organizations that do not continually improve their effectiveness.

- Critical Control 17
  - Penetration Tests and Red Team Exercises
- Conduct regular external and internal penetration tests

Attackers operate undiscovered in organizations

- Critical Control 18
  - Incident Response Capability
- Have written incident response procedures
- Devise time standards for reporting anomalous events

Attackers compromise systems and alter important data

- Critical Control 19
  - Data Recovery Capability
- Automatically back up on at least a weekly basis
- Data on backup media should be tested on a regular basis

Attackers exploit users and system admins via social engineering scams

- Critical Control 20
  - Security Skills Assessment and Appropriate Training to Fill Gap
- Develop security awareness training

Infogressive, Inc.
Aggressive Information Security

Offense Must Inform Defense

http://www.sans.org/critical-security-controls/